Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A method for concealing a parameter transferred between a first and second device, comprising:

generating, by the first device, a control signal and a parameter signal;

encrypting or hashing by the first device a portion of the control signal with the parameter signal to generate an encrypted or hashed parameter signal and control signal;

transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal;

receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal;

using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal; and

generating by the second device a destination parameter signal depending upon a comparison of the control signal and the decrypted or inversely transformed control signal.

2. (Currently Amended) The method of claim 1, ~~further characterized by~~ comprising:

generating by the first device a first key signal using the control signal; and

wherein encrypting or hashing comprises using the first key signal.

3. (Currently Amended) The method of claim 2, ~~further characterized by~~ comprising:

generating by the second device a second key signal using the control signal; and

generating by the second device the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the second key signal.

4. (Currently Amended) The method of claim 3, ~~further characterized by~~ comprising:

generating by the first device a key index signal;

generating by the first device a key variable signal;

transmitting by the first device to the second device the key index signal and the key variable signal;

receiving by the second device from the first device the key index signal and the key variable signal;

generating by the second device an intermediate key signal using the key index signal and a key table; and

generating by the second device the second key signal using the intermediate key signal and the key variable signal.

5. (Currently Amended) The method of claim 4, ~~further characterized by~~ comprising generating by the second device the second key signal from the intermediate key signal and the key variable signal using a hash function.

6. (Cancelled)

7. (Previously Presented) An apparatus for processing a concealed parameter received by a device, comprising:

a control logic block to receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal; and

an interface operation logic block operably coupled to the control logic block to decrypt or inversely transform the encrypted or hashed signal in accordance with the key index to generate a destination parameter signal.

8. (Currently Amended) The apparatus of claim 7, ~~further characterized by~~ comprising:

a key table module including indexed cryptographic keys, the key table module operably coupled to the control logic block, the key table module to generate a key signal using the control signal; and

an inverse transformation module operably coupled to the key table module and the control logic block, the inverse transformation module to generate the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the key signal.

9. (Currently Amended) The apparatus of claim 7, ~~further characterized by~~ comprising:

a key table module including indexed cryptographic keys, the key table module operably coupled to the control logic block, the key table module to generate an intermediate key signal using a key index signal received from the control logic block;

a key interface stage operably coupled to the key table module and the control logic block for generating a key signal using the intermediate key signal received from the key table module and a key variable signal received from the control logic block; and

an inverse transformation module operably coupled to the key interface stage and the control logic block, the inverse transformation module to generate the destination parameter signal by decrypting or inversely transforming the encrypted or hashed parameter signal using the key signal received from the key interface stage.

10. (Currently Amended) The apparatus of claim 9 ~~further characterized by~~ comprising a hash function stage operably coupled to the key interface stage, the hash function stage to generate the key signal from the intermediate key signal and the key variable signal.

11. (Previously Presented) The method of claim 1, wherein the control signal comprises a key index and the portion of the control signal comprises the key index.

12. (Previously Presented) The apparatus of claim 7, wherein the portion of the control signal comprises the key index.

13. (Currently Amended) A method for concealing a parameter transferred between a first and second device, ~~characterized by~~ comprising:

generating, by the first device, a control key signal comprising a key index;

using, by the first device, at least a portion of the control signal to obtain a first cryptographic key;

encrypting or hashing using the first cryptographic key, by the first device, a first signal to generate an encrypted or hashed signal;

transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal;

receiving, by the second device from the first device, the control signal and the encrypted or hashed signal;

using, by the second device, the key index from the control signal to obtain a second cryptographic key; and

decrypting or inversely transforming using the second cryptographic key, by the second device, the encrypted or hashed signal to provide a decrypted or inversely transformed signal.

14. (Previously Presented) The method of claim 13, wherein:

the first signal comprises a parameter signal and a portion of the control signal;

the decrypted or inversely hashed signal comprises a decrypted or inversely transformed portion of the control signal and a decrypted or inversely transformed parameter signal; and

the second device stores the decrypted or inversely transformed parameter signal depending on a comparison of a portion of the control signal received from the first device and the decrypted or inversely transformed portion of the control signal.

15. (Previously Presented) The method of claim 14, wherein the decrypted or inversely transformed portion of the control signal comprises the key index.

16. (Previously Presented) The method of claim 13, comprising:

transmitting, by the first device to the second device, a destination register signal;

receiving, by the second device from the first device, the destination register signal;

storing, by the second device, at least a portion of the decrypted or inversely transformed signal at a location determined in accordance with the destination register signal.

17. (Previously Presented) The method of claim 13 wherein using at least a portion of the control signal to obtain a first cryptographic key comprises using the key index as an index into a data memory to retrieve the first cryptographic key from the data memory.

18. (Previously Presented) The method of claim 13 wherein the key index comprises an index into a data memory that is used to retrieve the second cryptographic key from the data memory.